

58



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
 United States Patent and Trademark Office
 Address: COMMISSIONER FOR PATENTS
 P.O. Box 1450
 Alexandria, Virginia 22313-1450
 www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/727,104	11/29/2000	Dmitrii Loukianov	10559/383001/P10189	6820
20985	7590	02/23/2005	EXAMINER	
FISH & RICHARDSON, PC 12390 EL CAMINO REAL SAN DIEGO, CA 92130-2081			MOORTHY, ARAVIND K	
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 02/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/727,104

Applicant(s)

LOUKIANOV ET AL.

Examiner

Aravind K Moorthy

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 31 August 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-30 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-30 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 29 November 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. This is in response to the amendment on 31 August 2004.
2. Claims 1-30 are pending in the application.
3. Claims 1-30 have been rejected.

Response to Amendment

4. The examiner approves the "Brief Summary". No new matter has been added.

Response to Arguments

5. Applicant's arguments with respect to claims 1-30 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

6. Claims 1-5, 7-10 and 12-14 are rejected under 35 U.S.C. 102(e) as being anticipated by Kikinis U.S. Patent No. 6,289,389 B1.

As to claim 1, Kikinis discloses a cable modem comprising:

a controller, monitoring incoming cable modem transmissions for decryption keys, and monitoring conditions when the decryption keys are received [column 6, lines 33-47]; and

a register, storing the decryption keys only when the conditions meet the specified criteria [column 6, lines 33-47].

As to claim 2, Kikinis discloses that the cable modem includes a key processing element that causes the keys to be processed by software [column 6, lines 33-47].

As to claim 3, Kikinis discloses that the cable modem is a host migrated cable modem in which a host PC processes the keys [column 6, lines 33-47].

As to claim 4, Kikinis discloses that the register includes a write enable function, which allows information to be stored in the register only when the write enable function is in a specified condition [column 8, lines 6-45].

As to claim 5, Kikinis discloses that the controller allows operation with decryption keys only when the decryption keys are stored in the register [column 8, lines 6-45].

As to claim 7, Kikinis discloses that the register stores a plurality of decryption keys [column 7, lines 56-65]. Kikinis discloses each decryption key being uniquely associated with a specified identification number indicative of services for which the decryption key is applicable [column 7, lines 56-65].

As to claim 8, Kikinis discloses that the register further includes a write enable function, associated with each identification number, and which enables keys to be stored in the register associated with the write enable function only when the write enable function is in a specified state [column 7, lines 29-46].

As to claim 9, Kikinis discloses a method of controlling a cable modem, comprising:

monitoring an incoming cable stream for a decryption key [column 6, lines 33-47];

if a decryption key is present, then decrypting the decryption key in a host PC that is associated with the cable modem, but separate from the cable modem [column 6, lines 33-47]; and

allowing the decryption key to be used for decrypting the cable stream, only when the decryption key has been received in a specified way, otherwise not allowing the decryption key to be used for decrypting the cable stream [column 7, lines 29-46].

As to claim 10, Kikinis discloses that the specified way includes that the decryption key was received over the cable medium [column 6, lines 33-47].

As to claim 12, Kikinis discloses that the specified way includes that the decryption key is stored in a specified register [column 6, lines 33-47].

As to claim 13, Kikinis discloses storing the decryption key in a specified register when the allowing determines that the decryption key has been received in the specified way [column 8, lines 6-45].

Art Unit: 2131

As to claim 14 Kikinis discloses allowing the decryption key to be used only when the decryption key is stored in the register [column 8, lines 6-45].

7. Claims 22-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Beser U.S. Patent No. 6,442,158 B1.

As to claim 22, Beser discloses a system comprising:

a networked system of nodes, each node being uniquely controlled according to a unique identifier; at least one secure controller, the secure controller including a capability of providing permission to the nodes individually, according to the unique identifier [column 13 line 66 to column 6 line 10];

wherein each node includes a secure event detection element capable of receiving an encryption key from the secure controller, and a memory, storing the encryption key only when specified conditions occur [column 13 line 66 to column 6 line 10].

As to claim 23, Beser discloses that each the node is a cable modem [column 6, lines 15-25].

As to claim 24, Beser discloses monitor, in a first unit, a data stream for incoming keys of a specified format [column 13 line 66 to column 6 line 10]. Beser discloses sending the keys to another unit, other than the first unit, for decryption [column 13 line 66 to column 6 line 10]. Beser discloses enabling use of the keys only when the keys are received from the data stream in a specified way [column 13 line 66 to column 6 line 10].

As to claim 25, Beser discloses that the stream is a stream of cable modem information [column 6, lines 15-25].

As to claim 26, Beser discloses that the keys are DES encryption keys [column 13 line 66 to column 6 line 10].

As to claim 27, Beser discloses storing the keys in a specified location when they are received in the specified way [column 15, lines 15-62].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kikinis U.S. Patent No. 6,289,389 B1 as applied to claim 1 above, and further in view of McBride U.S. Patent No. 6,292,899 B1.

As to claim 6, Kikinis does not teach that the register includes a key destroy function, which allows a decryption key stored in the register to be marked as an invalid key, and prevents the key from being used for subsequent operations.

McBride teaches a register that includes a key destroy function. McBride teaches that it a decryption key stored in the register to be marked as an invalid key. McBride teaches that it prevents the key from being used for subsequent operations [column 6, lines 41-45].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Kikinis so that the register would have included a

key destroy function. The decryption key stored in the register would have been marked as an invalid key that would have prevented the key from being used for subsequent operations.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Kikinis by the teaching of McBride because it prevents unauthorized users to have access to encrypted information [column 2, lines 25-29].

9. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kikinis U.S. Patent No. 6,289,389 B1 as applied to claim 9 above, and further in view of Shimizu et al U.S. Patent No. 6,684,198 B1.

As to claim 11, Kikinis does not teach that the specified way includes that the decryption key was received associated with a particular service ID.

Shimizu et al teaches decryption keys that are associated with a particular service ID [column 2, lines 48-56].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Kikinis so that the decryption keys were associated with the service ID.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Kikinis by the teaching of Shimizu et al because it prevents unauthorized copying of program data [column 1, lines 64-67].

10. Claims 15-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kikinis U.S. Patent No. 6,289,389 B1 as applied to claim 9 above, and further in view of Choquet et al U.S. Patent No. 6,684,198 B1.

As to claims 15-17, Kikinis does not teach that the specified way includes requiring the decryption key to meet each of a plurality of specified rules. Kikinis does not teach that the specified rules include key writing to a decryption engine being normally disabled. Kikinis does not teach that at least one of the specified rules defines that the cable modem only receives messages on the cable that are addressed to the specified cable modem, and disregards messages which are addressed to other than specified cable modem.

Choquet et al teaches decryption keys to meet specified rules. Choquet et al teaches that the specified rules include key writing to a decryption engine being normally disabled. Choquet et al teaches that at least one of the specified rules defines that a modem only receives messages on the transmission medium that are addressed to the specified modem, and disregards messages that are addressed to other than specified modem [column 9, lines 33-50].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Kikinis so that the decryption keys would have had to meet specified rules. The specified rules would have included key writing to a decryption engine that was normally disabled. The cable modem would have only received messages on the cable that are addressed to the specified cable modem, and disregarded messages that are addressed to other than specified cable modem.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Kikinis by the teaching of Choquet et al because it

Art Unit: 2131

provides a messaging system that does not require the assignment of new system addresses and is immune to aliasing and false triggering [column 4, lines 6-17].

11. Claims 18-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kikinis U.S. Patent No. 6,289,389 B1 and Choquet et al U.S. Patent No. 6,684,198 B1 as applied to claim 15 above, and further in view of Doyle et al U.S. Patent No. 6,438,550 B1.

As to claim 18-20, the Kikinis-Choquet combination does not teach that at least one of the specified rules include that a specified service ID for specified key ring material causes key write capability to be enabled for the that specified service ID. The Kikinis-Choquet combination does not teach that an additional rule that disables key write for the service ID after key ring material is written to a storage area associated with the service ID. The Kikinis-Choquet combination does not teach that an additional rule that disables key write for the service ID, for specified time after writing the key ring material.

Doyle et al teaches a specified service ID for specified key ring material causes key write capability to be enabled for the that specified service ID. Doyle et al teaches a rule that disables key write for the service ID after key ring material is written to a storage area associated with the service ID. Doyle et al teaches a rule that disables key write for the service ID, for specified time after writing the key ring material [column 9, lines 24-67].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Kikinis-Choquet combination so that a specified service ID for specified key ring material caused key write capability to be enabled for the that specified service ID. There would have been a rule that disabled key write for the service ID after key ring material is written to a storage area associated with the service ID.

There would have been a rule that disabled key write for the service ID, for specified time after writing the key ring material.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Kikinis-Choquet combination by the teaching of Doyle et al because it allows client authentication to various servers and to allow access to configuration information for various software applications at whatever client computer a user may access [column 2, lines 17-21].

12. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kikinis U.S. Patent No. 6,289,389 B1 and Choquet et al U.S. Patent No. 6,684,198 B1 as applied to claim 15 above, and further in view of Lerner et al U.S. Patent No. 6,157,722.

As to claim 21, the Kikinis-Choquet combination does not teach that at least one of the specified rules include that the cable modem receives key ring material, writes the key ring material, and then destroys the key ring material.

Lerner et al teaches at least one of the specified rules include that a modem receives key ring material, writes the key ring material, and then destroys the key ring material [column 9, lines 27-34].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Kikinis-Choquet combination so that one of the specified rules included that a cable modem received key ring material, wrote the key ring material, and then destroyed the key ring material.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Kikinis-Choquet combination by the teaching of

Lerner et al because it prevents unauthorized access to the content of the communications [column 2, lines 45-57].

13. Claims 28-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beser U.S. Patent No. 6,442,158 B1 as applied to claim 24 above, and further in view of McBride U.S. Patent No. 6,292,899 B1.

As to claims 28-30, Beser does not teach that the keys are enabled for use only when they are stored in the specified location. Beser does not teach enabling writing only when specified conditions occur. Beser does not teach enabling specified keys to be destroyed.

McBride teaches keys that are enabled for use only when they are stored in the specified location. McBride teaches enabling writing only when specified conditions occur [column 5, lines 40-67]. McBride teaches enabling specified keys to be destroyed [column 6, lines 41-45].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Beser so that the keys can only be used when they are stored in the volatile key apparatus. Writing the keys to memory would have only took place when specified conditions occur. Specified keys would have been destroyed if unauthorized users were trying to intercept the decryption keys.


It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Beser by the teaching of McBride because it prevents unauthorized users to have access to encrypted information [column 2, lines 25-29].

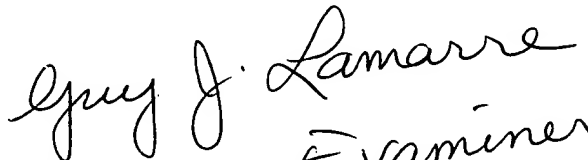
Conclusion

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy 
February 17, 2005


Primary Examiner